UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/042,652	01/08/2002	Jeffrey Bruce Lotspiech	ARC920010090US1	7388

7590 04/14/2006

John L. Rogitz
Rogitz & Associates
750 B Street, Suite 3120
San Diego, CA 92101

EXAMINER	
BERGER, AUBREY H	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 04/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/042,652
Filing Date: January 08, 2002
Appellant(s): LOTSPIECH ET AL.

John Rogitz
Registration No. 33,549
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 1/19/06 appealing from the Office action mailed 1/13/06.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is incorrect. A correct statement of the status of the claims is as follows:

This appeal involves claims 1, 3-16, 23-25, and 28-48.

The terminal disclosure submitted regarding claims 17-22 was not accepted.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

20020083319	Ishiguro et al.	06-2002
6691149	Yokota et al.	02-2004
6690795	Richards	02-2004
20010029581	Knauft	10-2001

(9) Grounds of Rejection

This rejection is fully set forth in prior Office Action mailed 1/13/06.

The following ground(s) of rejection are applicable to the appealed claims:

1. Claims 41-46 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Number 6,690,795 to Richards.

Regarding claim 41 and 43, Richards discloses a player/system, for decrypting streamed content (col. 2, lines 42-44; col. 1, lines 21-23), comprising: at least one device key K_d/UEV (fig. 14), means for decrypting a session key K_s/CAK, using the device key K_d/UEV, means for decrypting a channel unique key K_{cu}/CCK, using at least the session key K_s/CAK, and means for deriving a title key K_T/PK, using at least the channel unique key K_{cu}/CCK, the title key K_T/PK, being useful for decrypting content (fig. 14).

Regarding claim 42, Richards discloses the player/system, of claim 41, wherein the content is multicast to the player (col. 1, lines 13-18).

Regarding claim 44, Richards discloses a computer program device comprising: a computer program storage device including a program of instructions usable by a

computer (col. 2, line 63), comprising: logic means for receiving private information I_u /UEV register (fig. 14) upon registration with a content provider, logic means for subscribing to at least one content channel provided by the content provider (col. 3, lines 7-12), logic means for receiving at least one encrypted channel key K_c/control channel key (fig. 14), at least partially in response to subscribing to the channel, logic means for deriving the channel key K_c/control channel key, using the information I_u/UEV, and logic means for using at least the channel key K_c/control channel key, to decrypt content streamed over the channel (fig. 14).

Regarding claim 45, Richards discloses the computer program device of claim 44, further comprising: plural device keys K_d/customer code, logic means for receiving at least one session key block/DES (col. 21 lines 31-32), logic means for deriving at least one session key K_s/segment key, from the session key block using at least one device key K_d/customer code (fig. 8, #58).

Regarding claim 46, Richards discloses the computer program device of claim 45, further comprising: logic means for using the session key K_s/segment key, and channel key K_c/control channel key, to derive a channel unique key K_{cu}/channel access key, and logic means for using the channel unique key K_{cu}/channel access key, to decrypt a title key K_T/program key, useful for decrypting the content (fig. 27 & 28).

2. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Number 6,691,149 to Yokota et al (Yokota) and further in view of U.S. Patent Application Publication Number 2002/0083319 to Ishiguro et al (Ishiguro).

Regarding claim 1, Yokota discloses a method for securely transmitting multicast data (col. 5, lines 37-42), comprising: encrypting at least one title T/content, with at least title key K_T /contents key, and encrypting the title key K_T/contents key, with at least one channel-unique key K_{cu}/storage key (col. 9, lines 33-37), using at least one encryption function S/DES (col. 9, lines 14-16), to render a multicast data channel encrypted as $S_{Kcu}(K_T)$, $S_{KT}(T)$, (fig. 1, # 22).

Yokota lacks a channel-unique key that is a result of a combination of a concatenation of the channel key and session key. However, Ishiguro teaches wherein the channel-unique key K_{cu}/e, is the result of a combination of a channel key K_c/e1, and a session key K_s/e2, wherein the combination is a hash function of a concatenation of the channel key K_c/e1, and session key K_s/e2, (¶ [0104]). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of either Yokota with the device of Ishiguro. One of ordinary skill in the art would have been motivated to perform such a modification to the device of Yokota because Ishiguro teaches combining the channel key/e1, and session key/e2, to form the channel-unique-key/e further improves the security of the authentication procedure and the security of transmitted information by preventing an unauthorized user from posing as an authorized user using a desired piece of electronic equipment (¶[0014] & fig. 7).

3. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication Number 2001/0029581 to Knauft and further in view of U.S. Patent Application Publication Number 2002/0083319 to Ishiguro et al (Ishiguro).

Regarding claim 1, Knauft discloses a method for securely transmitting multicast data comprising: encrypting at least one title T/data object, with at least title key K_T /symmetric session key, and encrypting the title key K_T/symmetric session key (fig. 5A, #502), with at least one channel-unique key K_{cu}/public program key (fig. 5A, #504), using at least one encryption function S, to render a multicast data channel encrypted as $S_{Kcu}(K_T)$, $S_{KT}(T)$, (fig. 5A, #514).

Knauft lacks a channel-unique key that is a result of a combination of a concatenation of the channel key and session key. However, Ishiguro teaches wherein the channel-unique key K_{cu}/e, is the result of a combination of a channel key K_c/e1, and a session key K_s/e2, wherein the combination is a hash function of a concatenation of the channel key K_c/e1, and session key K_s/e2, (¶ [0104]). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of either Knauft with the device of Ishiguro. One of ordinary skill in the art would have been motivated to perform such a modification to the device of Knauft because Ishiguro teaches combining the channel key/e1, and session key/e2, to form the channel-unique key/e further improves the security of the authentication procedure and the security of transmitted information by preventing an unauthorized user from posing as an authorized user using a desired piece of electronic equipment (¶[0014] & fig. 7).

4. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Number 6,690,795 to Richards and further in view of U.S. Patent Application Publication Number 2002/0083319 to Ishiguro et al (Ishiguro).

Regarding claim 1, Richards discloses a method for securely transmitting multicast data (fig. 1), comprising: encrypting at least one title T/program A (fig. 2, #2), with at least title key K_T/Segment Key (fig. 2, #2), and encrypting the title key K_T/Segment Key, with at least one channel-unique key K_{cu}/Customer_code (fig. 2), using at least one encryption function S/DES (col. 6, lines 8-10), to render a multicast data channel encrypted as $S_{Kcu}(K_T)$, $S_{KT}(T)$, (fig. 2, #9).

Richards lacks a channel-unique key that is a result of a combination of a concatenation of the channel key and session key. However, Ishiguro teaches wherein the channel-unique key K_{cu}/e, is the result of a combination of a channel key K_c/e1, and a session key K_s/e2, wherein the combination is a hash function of a concatenation of the channel key K_c/e1, and session key K_s/e2, (¶ [0104]). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of either Richards with the device of Ishiguro. One of ordinary skill in the art would have been motivated to perform such a modification to the device of Richards because Ishiguro teaches teaches combining the channel key/e1, and session key/e2, to form the channel-unique key/e further improves the security of the authentication procedure and the security of transmitted information by preventing an unauthorized

user from posing as an authorized user using a desired piece of electronic equipment (¶[0014] & fig. 7).

5. Claims 3-16, 23, and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over either Yokota, Knauft, or Richards as individually applied to claim 1 above, and further in view of U.S. Patent Application Publication Number 2002/0083319 to Ishiguro et al (Ishiguro).

Regarding claim 3, Yokota, Knauft, or Richards further disclose the method of claim 1 as modified above, wherein the combination is a hash function of a concatenation of the channel key K_c/e1, and session key K_s/e2, (Ishiguro, ¶ [0104]).

Regarding claim 4, Yokota, Knauft, or Richards further disclose the method of claim 2 as modified above, wherein the session key K_s/e2, is encrypted with at least a first encryption scheme B^R_{s1}/DES [Ishiguro, ¶ [0079], to render a session key block/sk2' (Ishiguro, ¶ [0105]).

Regarding claim 5, Yokota, Knauft, or Richards further disclose the method of claim 4 as modified above by Ishiguro, comprising providing at least one player with device keys K_d/license key (Ishiguro, fig. 4), to activate the player [Ishiguro, ¶ [0065]).

Regarding claim 6, Yokota, Knauft, or Richards further disclose the method of claim 5 as modified above by Ishiguro, comprising providing the player with the channel key K_c/e1 (Ishiguro, fig. 6).

Regarding claim 7, Yokota, Knauft, or Richards further disclose the method of claim 6 as modified above by Ishiguro, wherein at least one of the providing acts is undertaken in a point-to-point communication (Ishiguro, fig. 1).

Regarding claim 8, Yokota, Knauft, or Richards further disclose the method of claim 6 as modified above by Ishiguro, wherein at least one of the providing acts is undertaken as part of a broadcast (Ishiguro, ¶ [0105]).

Regarding claim 9, Yokota, Knauft, or Richards further disclose the method of claim 6 as modified above by Ishiguro, comprising providing the player with the session key block/sk2' (Ishiguro, fig. 6).

Regarding claim 10, Yokota, Knauft, or Richards further disclose the method of claim 9 as modified above by Ishiguro, wherein the player can determine the session key K_s/e2, from the session key block/sk2', using the device keys K_d/license key (Ishiguro, ¶ [0105]).

Regarding claim 11, Yokota, Knauft, or Richards further disclose the method of claim 10 as modified above by Ishiguro, comprising periodically refreshing the channel key K_c/e1, (Ishiguro, fig. 7, steps 48-51) to enforce subscriptions.

Regarding claim 12, Yokota, Knauft, or Richards further disclose the method of claim 10 as modified above by Ishiguro, comprising selectively updating the session key block [Ishiguro, ¶0128].

Regarding claim 13, Yokota, Knauft, or Richards further disclose the method of claim 12 as modified above by Ishiguro, comprising updating the session key block/sk2',

by encrypting an updated session key/e2, with at least the encryption scheme B^R_{s1}/DES (Ishiguro, ¶ [0079]).

Regarding claim 14, Yokota, Knauft, or Richards further disclose the method of claim 11 as modified above by Ishiguro, wherein a new channel key K_c'/e1, is encrypted with at least a second encryption scheme B^R_{s2}/n-bit block encryption (Ishiguro, ¶ [0241]).

Regarding claim 15, Yokota, Knauft, or Richards further disclose the method of claim 14 as modified above by Ishiguro, wherein the new channel key K_c'/e1, is sent in a message that is split (Ishiguro, fig. 7, steps 48-51).

Regarding claim 16, Yokota, Knauft, or Richards further disclose the method of claim 14 as modified above by Ishiguro, wherein the new channel key K_c'/e1, is refreshed using plural messages (Ishiguro, fig. 7, steps 48-51).

Regarding claim 23, Yokota, Knauft, or Richards discloses the method of claim 1, as modified above by Ishiguro, wherein the content is streamed to players (Richards, col. 2, lines 41-43).

Regarding claim 47, Yokota, Knauft, or Richards further disclose the method of claim 14 as modified above by Ishiguro, wherein the new channel key K_c'/e1, is sent in-band with the title T (Ishiguro, fig. 7).

Ishiguro lacks partitioning players not in a revoked set R into disjoint subsets and encrypting the session key with the subset keys.

6. Claims 24-25, 28-40 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Richards, and further in view of Ishiguro.

Regarding claim 24, Richards discloses a method for enforcing copy protection compliance and subscription compliance comprising: providing players with respective device keys K_d/customer code, useful for enabling copy protection compliance, and providing players with at least one channel key K_c/working key (control channel key), useful for enabling subscription compliance such that a player can decrypt content only if the player is both compliant with copy protection and the player is an active subscriber to a content channel (col. 4, lines 43-46; fig. 27 & 28); encrypting at least one title T/program A (fig. 2, #2), with at least title key K_T/Segment Key (fig. 2, #2), and encrypting the title key K_T/Segment Key, with at least one channel-unique key K_{cu}/Customer_code, using at least one encryption function S/DES (col. 6, lines 8-10), to render a multicast data channel encrypted as $S_{Kcu}(K_T)$, $S_{KT}(T)$, (fig. 2, #9)

Richards lacks a channel-unique key that is a result of a combination of a concatenation of the channel key and session key. However, Ishiguro teaches wherein the channel-unique key K_{cu}/e, is the result of a combination of a channel key K_c/e1, and a session key K_s/e2, wherein the combination is a hash function of a concatenation of the channel key K_c/e1, and session key K_s/e2, (¶ [0104]). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of either Richards with the device of Ishiguro. One of ordinary skill in the art would have been motivated to perform such a modification to the device of Richards because Ishiguro teaches combining the channel key/e1, and session key/e2, to form

the channel-unique key/e further improves the security of the authentication procedure and the security of transmitted information by preventing an unauthorized user from posing as an authorized user using a desired piece of electronic equipment (¶[0014] & fig. 7).

Regarding claim 25, Richards discloses the method of claim 24 as modified above by Ishiguro, wherein the content is streamed to players (Richards, col. 2, lines 41-43).

As per claims 28-37, 39-40, and 48 all claimed limitations have been addressed and/or cited as set forth above corresponding to claims 2-12, 15-16, and 48 respectively.

Regarding claim 38, Richards discloses the method of claim 35 as modified above by Ishiguro, wherein the new channel key $K_c'/e1$, is refreshed by encrypting a new channel key $K_c'/e1$, with at least one encryption scheme (Ishiguro, fig. 7, steps 48-51).

(10) Response to Argument

The Appellant argues (page 5, ¶3):

However, the program key Pk of Richards is useless for decrypting content, because it is used to derive the segment key Sk.

The program key Pk of Richards is required to access the session key. Therefore, the program key Pk is "useful" in the sense that the program key is required to access the segment key Sk which encrypts/decrypts the content, (Richards, col. 7, lines 14-16; col. 10, lines 12-13; col. 11, lines 21-22; fig. 14, #152-165; col. 17, lines 44-48).

The Appellant argues (page 5, ¶4):

Additionally, Appellant notes that the "name of the game is the claim." The Federal Circuit has held that claims must be interpreted both in light of the specification and in light of surrounding claims. With this in mind, note that when Appellant recites an intermediate key in terms of its relationship with the ultimate decryption of content, Appellant has carefully selected different words to distinguish one from the other. That is why Claim 44 refers to an intermediate key Kc that is used "to decrypt content streamed over the channel", signaling that while Kc is used in the decryption process it cannot be "useful in decrypting content" itself.

In response to appellant's argument that the references fail to show certain features of appellant's invention, it is noted that the features upon which appellant relies (i.e., intermediate key Kc) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Additionally, the examiner has given the term "channel" key a plain and ordinary meaning according to one of ordinary skill in the encryption art. Accordingly, the control channel key CCK of Richards is "at least" used to decrypt the content, (Richards, fig. 14, #138-165; col. 17, lines 54-61).

The Appellant argues (page 6, ¶2):

As a further reason to reverse, consider that the element in Richards relied on for the claimed "session key" – the channel access key CAK – does not appear to change.

In response to appellant's argument that the references fail to show certain features of appellant's invention, it is noted that the features upon which appellant relies (i.e., the session key changing) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

The Appellant argues (page 6, ¶2):

The term "session key" plainly implies a key that is unique to a session. While the examiner dismisses "session" as a mere "title" that safely can be ignored particularly since it is "not defined in the claim".

The examiner has given the term session key a plain and ordinary meaning to one of ordinary skill in the encryption art. There is nothing in the claim to indicate use of a session and a corresponding key. The appellant only claims use of a channel and key. The channel is broadly interpreted as a communication path.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., the use of a session and a corresponding key) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from

the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

The Appellant argues (page 6, ¶3):

Richards does not state when the components are received or combined, much less that anything occurs upon registration.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., components are combined) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

The Appellant argues (page 7, ¶1):

Nowhere does Richards support the allegation that its control channel key CCU is received in response to subscribing channel.

However, Richards discloses "for a customer to obtain access to data carried by this dedicated channel, the customer must obtain the Control Channel Key, hence explaining the term CCK for Control Channel Key", (Richards, col. 11, lines 30-33).

The Appellant argues (page 7, ¶2):

While claim 45 inherits the patentability of claim 44, the rejection of it is based on another wave of the wand to conjure something out of Richards that isn't there, this time alleging that a session block is in Richards.

However, Richards discloses the use of television signals and triple-DES encryption, (col. 21, lines 11-18 & 25-30). The appellant is not specifically identifying features that are not taught, but rather asserts that a "session block" is not taught.

The Appellant argues (page 7, ¶3):

The examiner has been reminded that rejections should be strictly confined to the best available art. Cumulative rejections should be avoided, MPEP §706.02. The examiner has brushed aside the reminder. Appellant regrets the resulting inconvenience to the Board.

The Appellant is reminded that there are no limits to the number of rejections. The examiner identified the claims are broad and therefore applied multiple rejections.

The Appellant argues (page 7, ¶4):

The session keys appear to be generated in the DVD and thus function more like device keys, but in any event Ishiguro et al. does not even mention the word "channel" anywhere in its text.

However, Ishiguro, page 7, paragraph 104, teaches the session/channel is "unique" since identification ID1 and ID2 are concatenated to derive the common session key that is specific to two devices, (page 6, ¶[0088-0089]).

The Appellant argues (page 8, ¶1):

Ishiguro et al. has been proposed to be combined with Yokota et al., but no reference-specific analysis of why it would be obvious to combine the secondary reference with the very different primary reference has been offered.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the examiner has made a case of prima facie by supplying motivation (Ishiguro, ¶[0014]).

The Appellant argues (page 8, ¶3):

The session keys appear to be generated in the DVD and thus function more like device keys, but in any event Ishiguro et al: does not even mention the word "channel" anywhere in its text.

However, Ishiguro, page 7, paragraph 104, teaches the session/channel is "unique" since identification ID1 and ID2 are concatenated to derive the common session key that is specific or unique, to two devices, (page 6, ¶[0088-0089]).

The Appellant argues (page 9, ¶1):

Ishiguro et al. has been proposed to be combined with Knauft, but no reference-specific analysis of why it would be obvious to combine the secondary reference with the very different primary reference has been offered.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the examiner has made a case of prima facie by supplying motivation (Ishiguro, ¶[0014]).

The Appellant argues (page 9, ¶3):

The session keys appear to be generated in the DVD and thus function more like device keys, but in any event Ishiguro et al. does not even mention the word "channel" anywhere in its text.

However, Ishiguro, page 7, paragraph 104, teaches the session/channel is "unique" since identification ID1 and ID2 are concatenated to derive the common session key that is specific to two devices, (page 6, ¶[0088-0089]).

The Appellant argues (page 10, ¶1):

Ishiguro et al. has been proposed to be combined with Knauft, but no reference-specific analysis of why it would be obvious to combine the secondary reference with the very different primary reference has been offered.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the examiner has made a case of prima facie by supplying motivation (Ishiguro, ¶[0014]).

The Appellant argues (page 10, ¶3; page 11, ¶1; page 11, ¶2):

It does not appear that the device keys of Ishiguro et al. are used to activate the player, as otherwise recited in Claim 5, nor does anything resembling a key block, much less a session key block, appear in the secondary reference as otherwise recited in Claim 9.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., key block or session key block) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Additionally, the Appellant has provided mere allegations and has not specifically addressed or argued features taught in the reference.

As best understood by the Appellants arguments, Ishiguro teaches the use of block encryption and DES, (¶[0240]).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

(12) Conclusion

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

AHB

AHB 4/10/06

Conferees:

Kim Vu KV

Christopher Revak

CHRISTOPHER REVAK
PRIMARY EXAMINER